BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Digital Output Protection Technology	)	
and Recording Method Certifications:	)	MB Docket No. 04-59
	)	
SmartRight	)	
	)	

COMMENTS OF SMARTRIGHT TO THE PETITION FOR PARTIAL RECONSIDERATION AND CLARIFICATION BY THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., ET AL

Thomson Inc. ("Thomson"), on behalf of itself and its SmartRight Partners ("SmartRight"),[1] submits these Comments on the Petition for Partial Reconsideration and Clarification filed by the Motion Picture Association of America, Inc. and its member studios ("MPAA Parties")[2] to the Commission's August 4, 2004 Order.[3] Specifically, SmartRight seeks to: (1) clarify that the SmartRight system provides completely secure protection for digital broadcast content from mass indiscriminate redistribution over the Internet, even without proximity controls; and (2) underscore SmartRight's voluntary commitment to implement proximity controls in its initial deployment, pending the outcome of discussions with MPAA and

[1] SmartRight's partners include: Axalto, Gemplus S.A., Micronas, Nagravision S.A., Pioneer Corporation, SCM Microsystems, and ST Microelectronics N.V. and Thomson.

[2] *In the Matter of Digital Output Protection Technology and Recording Method Certifications*, Petition for Partial Reconsideration and Clarification by the Motion Picture Association of America, Inc., Metro-Goldwyn-Mayer Studios, Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, The Walt Disney Company, and Warner Bros. Entertainment Inc., MB Docket Nos. 04-55, *et. al.* (Sept. 13, 2004) ("*MPAA Petition*").

[3] *In the Matter of Digital Output Protection Technology and Recording Method Certifications*, Order, MB Docket Nos. 04-55, *et al.*, FCC 04-193 (rel. Aug. 12, 2004) ("*Certification Order*").

its member studios concerning conditions for remote access and the resolution of related outstanding issues in the Commission's Broadcast Flag FNPRM.[4]

I. THE SMARTRIGHT SYSTEM FULFILLS THE COMMISSION'S GOAL OF PROTECTING DIGITAL BROADCAST TELEVISION CONTENT FROM MASS INDISCRIMINATE REDISTRIBUTION OVER THE INTERNET

The SmartRight system fulfills the Commission's stated goal of protecting digital broadcast television content from mass indiscriminate redistribution over the Internet. As detailed in the *SmartRight Certification*,[5] unlike other encryption-based technologies that use a "chain of protection" approach wherein marked content is successively encrypted and decrypted within the personal digital network, the SmartRight system, through the use of redundant, state-of-the-art security mechanisms,[6] provides a secure and seamless blanket of protection from the moment the content is received, and throughout its movement within a consumer's secure domain of devices known as the PPN.[7] Once "flagged" content has been encrypted by the SmartRight system, it remains encrypted and cannot be redistributed to anyone over the Internet, including to those with their own SmartRight Personal Private Network, without retaining that encryption.

---

[4] *In the Matter of Digital Broadcast Content Protection*, Report and Order and Further Notice of Proposed Rulemaking, MB Docket No. 02-230, 18 FCC Rcd 23550 (2003) ("*Broadcast Flag Report and Order and FNPRM").*

[5] *In the Matter of Digital Output Protection Technology and Recording Method Certifications: SmartRight*, MB Docket No. 04-59 (March 1, 2004) ("*SmartRight Certification*").

[6] These include the use of smart card renewability, device limitations, interactive device authentication, multi-level device revocation, 112-bit Triple DES for content scrambling, 128-bit AES for individual device communications and identification, 1024 or 2048-bit RSA for authentication and SHA1 hash function for verification. *SmartRight Certification* at 16.

[7] The PPN is a limited set of devices, belonging to a family or an authorized network domain, which are linked through wired or wireless digital connections.

As the Commission itself correctly notes in its *Certification Order*, once received, "protected content cannot be accessed in a usable format on any device outside the specific PPN in which it was encrypted, [even] on devices linked to other SmartRight PPNs."[8] Outside the Personal Private Network, including in the case of attempted mass indiscriminate redistribution over the Internet, digital content encrypted by the SmartRight system is *unviewable* on any device that has not been linked with the originating PPN by the PPN owner.[9] In this manner, the SmartRight system ensures that the content it protects cannot be redistributed indiscriminately in any usable form.

SmartRight wishes to allay MPAA Parties' specific concern that, absent the inclusion of proximity controls,[10] "nothing prevents each SmartRight Personal Private Network ('PPN') from being used to indiscriminately redistribute broadcast television content to up to nine total strangers."[11]

As discussed in the *SmartRight Certification*, one of the patented security mechanisms featured in the SmartRight system is its ability to limit the size of the Personal Private Network, *i.e.*, by limiting the number of presentation devices.[12] Simply put, this mechanism employs the

---

[8] *Certification Order* at 58.

[9] SmartRight Partners, after discussions with the content community, agreed to require physical propagation of the PPN as part of its initial implementation. *See In the Matter of Digital Output Protection Technology and Recording Method Certifications: SmartRight*, Reply of SmartRight Applicants to the Opposition of the Motion Picture Association of America Inc., et al, MB Docket No. 04-59 (April 16, 2004) ("*SmartRight Reply to MPAA Opposition*") at 9.

[10] As discussed *infra*, SmartRight has committed to activate proximity controls on a voluntary basis in the SmartRight system's initial implementation.

[11] *MPAA Petition* at 9. SmartRight notes that, technically, this falls outside the Commission's explicitly stated goal of preventing *mass* indiscriminate redistribution." *See Certification Order* at 61 (emphasis added). *See also Broadcast Flag Report and Order and FNPRM* at 4.

[12] *See SmartRight Certification* at 16. Based on consultations with the content community, SmartRight will limit the number of presentation devices within a single PPN to 10. *See SmartRight Reply to MPAA Opposition* at 9, n.17.

SmartRight system's state-of-the-art key management system to create a single, unique "progenitor token" for every PPN. The progenitor token resides in the last installed smart card on the PPN, and is mandatory to add a new presentation device to a PPN. The progenitor token also is the mechanism that keeps track of, and ultimately limits, the number of presentation devices included on the PPN.

Whereas the SmartRight system, as certified, is capable of enabling remote propagation of the PPN over the Internet, in response to MPAA Parties' request, SmartRight agreed that, for purposes of its initial implementation, propagation of the SmartRight PPN will require the physical insertion of the PPN owner's smart card (containing the unique progenitor token) into the presentation device to be added.[13] Such a face-to-face-based mechanism, virtually by definition, effectively prevents the inclusion in the PPN of devices belonging to "total strangers."

II. SMARTRIGHT REMAINS COMMITTED TO IMPLEMENTING PROXIMITY CONTROLS ON AN INTERIM BASIS WHILE CONDITIONS FOR REMOTE ACCESS ARE DEVELOPED

As the Commission is aware, the SmartRight system – as certified to and approved by the Commission – includes the capability to enable consumers to access protected content on remote devices within their Personal Private Network, while still protecting that content from indiscriminate redistribution over the Internet.[14] In addition, the SmartRight system also includes a "local proximity control" feature which, when appropriately activated, can restrict, on a geographic basis, redistribution of Marked and Unscreened content.[15]

---

[13] *See SmartRight Reply to MPAA Opposition* at 9.

[14] *See SmartRight Certification* at 8, 12.

[15] *See SmartRight Certification* at 2, §§ 5.4 (technical specification description) and 9.12 (SmartRight license description). *See also, SmartRight Reply to MPAA Opposition*, Appendix A (which contains the SmartRight Adopter Agreement) at § 7.1.

While SmartRight believes that the availability of the SmartRight system's *secure* remote access capability ultimately will help drive consumer demand for DTV and the creative works that DTV delivers to the home, SmartRight is sensitive to the concern articulated by the MPAA[16] that deployment of remote access capability, at this time, raises numerous interrelated and complex business, legal and technical issues that require careful FCC consideration. Indeed, MPAA Parties' concern that certain digital output and recording technologies seeking approval by the Commission[17] did not sufficiently "localize" protected content, especially prior to the Commission's adoption of final criteria focusing on remote access to content, was a principal reason for MPAA Parties' initial opposition to these technologies, including the SmartRight system.

In response to these concerns, and after extensive and constructive discussions with MPAA, SmartRight agreed voluntarily to activate the SmartRight system's proximity controls, on an interim basis, in conformance with technical parameters that will limit redistribution of Marked and Unscreened content to networking within the proximity of the home.[18] Based on this

---

[16] *In the Matter of Digital Output Protection Technology and Recording Method Certifications: SmartRight*, Opposition To The Application of SmartRight by the Motion Picture Association of America Inc., Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, The Walt Disney Company, and Warner Bros. Entertainment Inc., MB Docket No. 04-59 (April 6, 2004) ("*MPAA Parties' Opposition")*.

[17] In addition to the SmartRight system, these included DTCP, TiVoGuard, WindowsMedia DRM and HelixDRM.

[18] The specific parameters of SmartRight's proximity controls were detailed in a May 28, 2004 *ex parte* letter submitted jointly by MPAA and Thomson and are restated here for the Commission's convenience:

> At a minimum, SmartRight local proximity detection will include:(i) setting the Internet Protocol (IP) packet header parameter Time to Live (TTL) to 3 in all transmitted IP packets of Marked or Unscreened Content output from a Covered Product source device; (ii) confirmation that any Internet Protocol (IP) packets of Marked or Unscreened Content received by a Covered Product sink device have an IP Time to Live (TTL) parameter value of no greater than 3; and (iii) confirmation by the Covered Product source device for any transmission of Marked or Unscreened Content (including over

and other commitments by SmartRight,[19] the MPAA dropped its opposition to the SmartRight system and supported its approval by the Commission.[20]

SmartRight's commitment to implement proximity controls was reiterated immediately and publicly upon the Commission's approval of the SmartRight system,[21] and remains fully in force today. Private discussions with the MPAA are now underway to determine under what conditions remote access to content can be permitted, and the full functionality of the SmartRight system can be exploited for the benefit of consumers. SmartRight is hopeful that a future private

---

> point-to-point wired connections) that one valid measurement of a Round Trip Time (RTT) of 7 milliseconds or less has been made between itself and the Covered Product sink device prior to completing the sink device's authentication request. Time to Live (TTL) is defined in Internet Standard RFC 791 STD 5.
>
> The measurement of Round Trip time (RTT) by a Covered Product source device will occur: (a) after power-up of the Covered Product source device when an active Covered Product sink device requests authentication; (b) when the last transmission of content-based packet traffic between a Covered Product source device and sink device has occurred more than 120 minutes prior; and (c) when the last successful RTT measurement of 7 milliseconds or less between a Covered Product source and sink device has occurred more than 24 hours prior.
>
> The determination of RTT will be measured using a cryptographically secure protocol to prevent any form of spoofing and to ensure that only the authenticating Covered Product sink device receiving the protected content can respond to the RTT measurement message. A Covered Product source device will attempt the measurement of RTT until it achieves a single valid measurement of 7 or fewer milliseconds or determines that this requirement cannot be met and completion of authentication is halted. Thus, the RTT measurement will be the minimum RTT value measured and not the average of all RTT values measured. Letter from C. Bradley Hunt, MPAA, and David Arland, Thomson, to Kenneth Ferree, FCC, MB Docket 04-59 (May 28, 2004) ("*MPAA-Thomson May 28, 2004 ex parte*") at 2.

This commitment was made with the understanding that, should future relaxation of these controls be appropriate (either pursuant to an agreement with content owners or FCC rules), such relaxation could be achieved without further Commission action. *See MPAA-Thomson May 28, 2004 ex parte* at 2. *See also* Letter from David Arland, Thomson, to Marlene Dortch, FCC, MB Docket 04-59 (June 23, 2004) at 2.

[19] *See MPAA-Thomson May 28, 2004 ex parte*. *See also SmartRight Reply to MPAA Opposition.*

[20] *See MPAA-Thomson May 28, 2004 ex parte* at 3.

[21] *See* Paul Gluckman, *Thomson Reaffirms Pledge to Impose SmartRight Proximity Controls*, Consumer Electronics Daily, August 30, 2004.

agreement on remote access might provide helpful guidance to the Commission as it continues its deliberations in the *Broadcast Flag FNPRM*.

III. CONCLUSION

SmartRight appreciates the opportunity to clarify the record regarding the SmartRight system's ability, with or without proximity controls, to fulfill the Commission's goal of protecting digital broadcast content from mass indiscriminate redistribution over the Internet. With discussions now underway to develop the conditions that permit remote access, SmartRight reaffirms its commitment to incorporate proximity controls on an interim basis.

Respectfully submitted,

THOMSON INC., ON BEHALF OF SMARTRIGHT

David H. Arland
Vice President, U.S. Corporate Communications
and Government Relations
Thomson Inc.
P.O. Box 1976, INH-430
Indianapolis, IN 46206-1976
(317) 587-4832

September 23, 2004

CERTIFICATE OF SERVICE

The undersigned hereby certifies that true and correct copies of the foregoing were served on the following individuals on September 23, 2004, both electronically and by first-class mail, postage pre-paid:

Jon A. Baumgarten
Proskauer Rose LLP
1233 Twentieth Street, N.W.
Suite 800
Washington, D.C. 20036

Bruce Boyden
Proskauer Rose LLP
1233 Twentieth Street, N.W.
Suite 800
Washington, D.C. 20036

David H. Arland